Citrix Workspace app for Android

Contents

About this release

January 25, 2022

What's new in 21.12.0

Support for Zebra workstation connect

With this release, we introduce compatibility with Zebra tablet features - desktop launcher and experience in desktop mode. The user experience of the Android tablet is mirrored on the client monitor with Zebra Workspace Connector.

For more information on managing the zebra device, see Manage Zebra Android devices in the Citrix Endpoint Management documentation.

Recommendations and notes (Android 12, HTTPS)

- Citrix Workspace app for Android 21.11.0 supports Android 12.
- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

Fixed issues in 21.12.0

This release addresses issues that help to improve overall performance and stability.

Known issues in 21.12.0

No new known issues have been observed in this release.

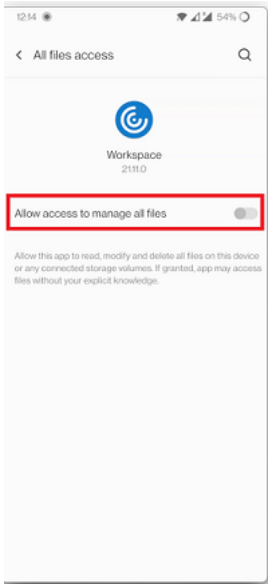
Earlier releases

This section provides information on the new features and fixed issues in the previous releases that we support as per the Lifecycle Milestones for Citrix Workspace app.

21.11.0

Allow access to manage all files

With this release, we have introduced the permission option – **Allow access to manage all files**. We recommend that you enable this permission for optimal performance. Your files remain secure.



Recommendations and notes (Android 12, HTTPS)

- Citrix Workspace app for Android 21.11.0 supports Android 12.
- If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

Feature limitation

After migrating to Citrix Workspace from StoreFront, the screen flickers momentarily while tapping the **Next** button on the Pendo guide.

Fixed issues

- Smart card intergration fails with Citrix workspace app. With this issue fixed, you can use personal identity verification (PIV) and common access card (CAC) smart cards for authentication. [RFANDROID-8970]

> **Note:**
>
> To know the existing issues within the product, see Known issues section.

21.10.0

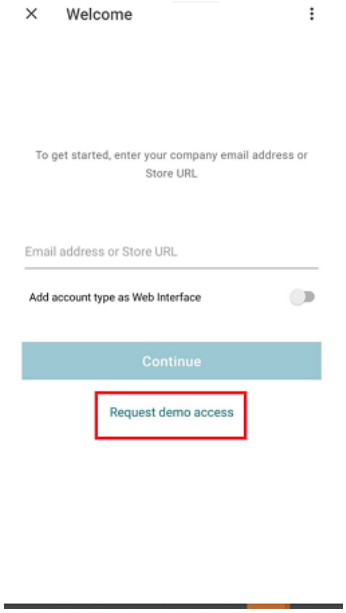
Free demo access

Trying out the Citrix Workspace experience on mobile devices just got easier. Potential users and anyone interested now have free demo access of the Citrix Workspace app for Android.

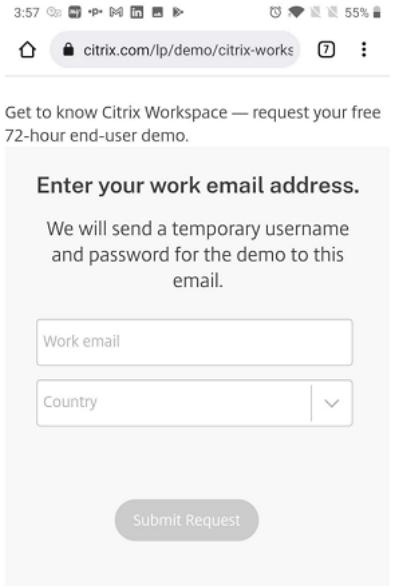
You can get to know about Citrix Workspace app by requesting a free 72-hour trial.

To request free demo access,

1. Tap **Request demo access** on the **Citrix Workspace app Sign in** screen.



2. The Citrix request demo access webpage appears.
3. Enter your required details like name, company, address, phone number, city, work email address, and then tap **Submit Request**.



4. You receive a temporary user name and password on your work email address. Enter the temporary user name and password on the **Sign in** screen.

You now have free demo access to Citrix Workspace app for 72 hours.

Recommendations and notes (Android 12, HTTPS)

- Citrix Workspace app for Android 21.10.0 supports Android 12.
- If you're on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

Fixed issues

This release addresses issues that help to improve overall performance and stability.

> **Note:**
>
> To know the existing issues within the product, see Known issues section.

Known issues

Known issues in 21.7.5

You might see an Auto Client Reconnect (ACR) dialog box when the network disconnects and reconnects during a session through a VDA. Tap Connect to resume the session. [RFANDROID-3574]

Known issues in 21.4.0

No new known issues have been observed in this release.

> **Note:**
>
> When you are enrolled in Work profile in Citrix Workspace app, launching your sessions using the Chrome browser from an ICA file in Personal profile no longer works. However, the issue is not present with Citrix Secure Web on adding the ICA file URL in the exclusion list.

Known issues in 21.2.1

When you launch an app that uses your location, the **Google Play policy** dialog box appears even after setting the location permissions to Allow on Citrix Workspace app. The issue occurs on Android Version 9 and earlier. [RFANDROID-7893]

Known issues in 20.3.0

- On a Samsung DeX device, you might not be able to cancel USB device redirection if you dismiss the permission prompt without clicking the **Cancel** button. [RFANDROID-5397]

Known issues in 20.2.0

- Attempts to launch a session fail with an error message when you disable the **Session Reliability** policy on an SSL-enabled VDA. [RFANDROID-5065]
- Attempts to launch SaaS apps might fail in a session running in Kiosk mode in cloud deployments. [RFANDROID-5137]
- Client reconnection attempts do not work and the following error message appears:

  "General problem, try connecting again."

  The issue occurs on Citrix Gateway-configured stores if the **Session Reconnect** option is disabled and the **Automatic Client Reconnect** option is enabled on the Controller.

  [RFANDROID-5138]
- Attempts to reconnect fail when you click **Connect** in the **Auto Client Reconnect** dialog. The issue occurs in sessions connected to Citrix XenApp and XenDesktop Version 7.6 CU 8. [RFANDROID-5151]

Known issues in 20.1.5

- In a multiple store-cloud setup, deleting a store might not remove the Store details. The Store remains listed until the user removes the Workspace app from the **Recent** tab. [RFANDROID-5043]

Feature preview

Feature previews are available for customers to use in their non-production or limited production environments, and to give them an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix may or may not act on feedback based on its severity, criticality, and importance.

Third-party notices

Citrix products often include third-party code licensed to Citrix for use and redistribution under an open source license. To better inform its customers, Citrix publicizes open source code included within Citrix products in an open source licensed code list.

For information about Open Source Licensed Code, see Open Source Licensed Code.

Citrix Workspace app might include third-party software licensed under the terms defined in the following document:

Citrix Workspace app for Android Third-Party Notices

Prerequisites for installing

September 16, 2020

System requirements and compatibility

Device requirements

Citrix Workspace app for Android supports Android 7.x (Nougat), 8.x (Oreo), 9.x (Pie), 10.x (Android Q) and 11 (Android R).

For best results, update Android devices to the latest Android software.

Citrix Workspace app supports launching sessions from Workspace for Web, when the web browser works with Workspace for Web. If launches do not occur, configure your account through Citrix Workspace app directly.

> **Important:**
>
> If a Tech Preview version of Citrix Workspace app for Android is installed, uninstall it before installing the new version.

Server requirements

StoreFront:

- StoreFront 2.6 or later

  Provides direct access to StoreFront stores. Citrix Workspace app for Android also supports prior versions of StoreFront.

- StoreFront configured with a Workspace for website

  Provides access to StoreFront stores from a web browser. For the limitations of this deployment, see the StoreFront documentation.

You must enable the rewrite policies provided by Citrix Gateway.

Citrix Virtual Apps and Desktops (any of the following products):

- Citrix Virtual Apps 7.5 or later
- XenApp 6.5 for Windows Server 2008 R2
- Citrix Virtual Apps and Desktops 7.x or later

Connections, certificates, and authentication

Citrix Workspace app supports HTTP, HTTPS, and ICA-over-TLS connections to a Citrix Virtual Apps server through any one of the following configurations.

For LAN connections:

- StoreFront 2.6 or later
- XenApp Services (formerly Program Neighborhood Agent) site.

For secure remote connections (any of the following products):

- Citrix Gateway 11 and later (including VPX, MPX, and SDX versions)

TLS Certificates

When securing remote connections using TLS, the mobile device verifies the authenticity of the remote gateway's TLS certificate against a local store of trusted root certificate authorities. The device automatically recognizes commercially issued certificates (such as VeriSign and Thawte) provided the root certificate for the certificate authority exists in the local keystore.

Private (Self-signed) Certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the mobile device to successfully access Citrix resources using Citrix Workspace app for Android.

> **Note:**
>
> When the remote gateway's certificate cannot be verified upon connection (because the root certificate is not included in the local keystore), an untrusted certificate warning appears. If a user selects to continue through the warning, a list of applications is displayed; however, application fails to launch.

Wildcard Certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app for Android supports wildcard certificates.

Intermediate Certificates and Citrix Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway server certificate. See Knowledge Center article that matches your edition of the Citrix Gateway:

CTX114146 and CTX124937

Joint Server Certificate Validation Policy

Citrix Workspace app for Android has a stricter validation policy for server certificates.

> **Important:**
>
> Before installing this version of Citrix Workspace app for Android, confirm that the certificates at the server or Citrix Gateway are correctly configured as described here. Connections might fail if:
>
> - the server or Citrix Gateway configuration includes a wrong root certificate.
> - the server or Citrix Gateway configuration does not include all intermediate certificates.
> - the server or Citrix Gateway configuration includes an expired or otherwise invalid intermediate certificate.
> - the server or Citrix Gateway configuration includes a cross-signed intermediate certificate.

When validating a server certificate, Citrix Workspace app for Android uses **all** the certificates supplied by the server (or Citrix Gateway) when validating the server certificate. It then also checks that the certificates are trusted. If the certificates are not all trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or Citrix Gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Workspace app for Android connection to fail.

Suppose that a Citrix Gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Workspace app for Android:

- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Example Root Certificate”

Then, Citrix Workspace app for Android checks that all these certificates are valid. Citrix Workspace app for Android also checks that it already trusts “Example Root Certificate”. If Citrix Workspace app for Android does not trust “Example Root Certificate,” the connection fails.

> **Important**
>
> Some certificate authorities have more than one root certificate. If you require this stricter validation, make sure that your configuration uses the appropriate root certificate. For example, there are currently two certificates (“DigiCert”/”GTE CyberTrust Global Root,” and “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”) that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available (“DigiCert Baltimore Root”/”Baltimore CyberTrust Root”). If you configure “GTE CyberTrust Global Root” at the

> gateway, Citrix Workspace app for Android connections on those user devices will fail. Consult the certificate authority's documentation to determine which root certificate should be used. Also note that root certificates eventually expire, as do all certificates.
>
> **Note:**
>
> Some servers and Citrix Gateway never send the root certificate, even if configured. Stricter validation is then not possible.

Now suppose that a gateway is configured by using these valid certificates. This configuration, omitting the root certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Then, Citrix Workspace app for Android uses these two certificates. It will then search for a root certificate on the user device. If it finds one that validates correctly, and is also trusted (such as "Example Root Certificate"), the connection succeeds. Otherwise, the connection fails. This configuration supplies the intermediate certificate that Citrix Workspace app for Android needs, but also allows Citrix Workspace app for Android to choose any valid, trusted, root certificate.

Now suppose that a Citrix Gateway is configured by using these certificates:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Wrong Root Certificate"

Citrix Workspace app for Android reads the wrong root certificate, and the connection fails.

Some certificate authorities use more than one intermediate certificate. In this case, the Citrix Gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- "Example Server Certificate"
- "Example Intermediate Certificate 1"
- "Example Intermediate Certificate 2"

Some certificate authorities use a cross-signed intermediate certificate. This is intended for situations there is more than one root certificate, and an earlier root certificate is still in use at the same time as a later root certificate. In this case, there will be at least two intermediate certificates. For example, the earlier root certificate "Class 3 Public Primary Certification Authority" has the corresponding cross-signed intermediate certificate "VeriSign Class 3 Public Primary Certification Authority - G5."However, a corresponding later root certificate "VeriSign Class 3 Public Primary Certification Authority - G5" is also available, which replaces "Class 3 Public Primary Certification Authority." The later root certificate does not use a cross-signed intermediate certificate.

The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To), but the cross-signed intermediate certificate has a different Issuer name (Issued By). This dis-

tinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such "Example Intermediate Certificate 2").

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Avoid configuring the Citrix Gateway to use the cross-signed intermediate certificate, because it selects the earlier root certificate:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Example Cross-signed Intermediate Certificate" [not recommended]

It is not recommended to configure the Citrix Gateway by using only the server certificate:

- "Example Server Certificate"

When Citrix Workspace app for Android cannot locate all the intermediate certificates, the connection fails.

Authentication

> **Note:**
>
> RSA SecurID authentication is not supported for Citrix Secure Web Gateway configurations. To use RSA SecurID, use Citrix Gateway.

Citrix Workspace app for Android supports authentication through Citrix Gateway using the following methods, depending on your edition:

- No authentication (Standard and Enterprise versions only)
- Domain authentication
- RSA SecurID, including software tokens for Wi-Fi and non-Wi-Fi devices
- Domain authentication paired with RSA SecurID
- SMS Passcode (one-time PIN) authentication
- Smartcard authentication

Citrix Workspace app for Android now supports the following products and configurations.

Supported smart card readers:

- BaiMobile 3000MP USB Smart Card Reader

Supported smart cards:

- PIV cards
- Common Access Cards

Supported configurations:

- Smart card authentication to Citrix Gateway with StoreFront 2 or 3 and Citrix Virtual Apps and Desktops 7.x and later or XenApp 6.5 and later.

> **Note:**
>
> Other token-based authentication solutions can be configured using RADIUS. For SafeWord token authentication, see Configuring SafeWord Authentication.

Install, Upgrade

July 16, 2021

Upgrade

To upgrade to the latest Citrix Workspace app, do any of the following steps:

- Download the Citrix Workspace app from the Citrix Download page and install the app to upgrade from Citrix Receiver to Citrix Workspace app.
- Upgrade your Citrix Workspace app using Google Play.

For information about the features available in Citrix Workspace app for Android, see Citrix Workspace app Feature Matrix.

For the documentation of Citrix Receiver for Android, see Citrix Receiver.

HDX RealTime Media Engine

Citrix HDX RTME plug-in is embedded with the Citrix Workspace app installer.

The HDX RealTime Media Engine (RTME) is a plug-in to the Citrix Workspace app to support clear, crisp high-definition audio-video calls. You can seamlessly participate in audio-video or audio-only calls to and from HDX RealTime Media Engine users.

HDX RTME integrates Citrix Workspace app on the endpoint device and performs media processing on the user device, offloading the server for maximum scalability, minimizing network bandwidth consumption and ensuring optimal audio-video quality.

> **Note:**
>
> - HDX RTME for Citrix Workspace app for Android is supported only on Chromebooks with Intel Core Processor.
> - You must uninstall the existing version of HDX RTME to install the latest version available

> with the Citrix Workspace app.

Citrix Workspace app for Android does not support the following HDX RTME features:

- Camera encoding USB Video Class (UVC) 1.1.
- Device enumeration and switching from Skype for Business settings. Only default devices are used.
- G722.1C, RTAudio, and RTVideo codecs.
- Human interface devices, auto gain control, and Call Admission Control.
- In **Fallback** mode, webcam and audio devices are not available because of limitations in Citrix Workspace app for Android.

Enable HDX RTME from Citrix Workspace app:

By default, this setting is set to **Off**.

To enable the HDX RTME from Citrix Workspace app, go to **Settings** > **Advanced** and select **Enable RealTime Media Engine**.

For more information about the HDX RealTime Media Engine, see HDX RealTime Optimization Pack documentation.

Installing Citrix Workspace app on an SD card

Citrix Workspace app for Android is optimized for local installation on user devices. However, if devices have insufficient storage, users can install Citrix Workspace app for Android on an external SD card and mount it on the device to launch published apps on their mobile devices. This support is provided by default and no additional configuration is required.

To launch an app using the SD card, select the app from the list of Citrix Workspace app on the user device, and then select Move to SD card.

If users opt to install Citrix Workspace app for Android on an external SD card to launch apps, the following issues exist:

- Mounting a USB storage device while the SD card is mounted on the mobile device causes the SD card to become unavailable, and if apps were running, they stop running when the USB device is mounted.
- Some AppWidgets (such as the home screen widgets) are not available when an app is running from the SD card. After unmounting the SD card, users must restart the AppWidgets.

If users install Citrix Workspace app for Android locally on their user devices, they can move Citrix Workspace app for Android to the SD card when needed.

ProGuard enabled for security

We've ProGuard enabled to make Citrix Workspace for Android secure through obfuscation. ProGuard renames different parts of the code to prevent inspection of stack traces and makes the Workspace app secure. ProGuard also reduces the app size by shortening the names of app classes, methods, and fields.

Get started

January 31, 2022

While you create an account do the following:

1. In the **Address** field, enter the matching URL of your store, such as storefront.organization.com. Fill the other fields with necessary details.
2. Select the Citrix Gateway authentication method, such as enabling the security token.
3. Select the type of authentication, and then save the settings.
4. When you use automatic configuration, do any of the following:
    - enter the FQDN of a StoreFront server or Citrix Gateway.
    - use an email address to create an account.
5. When prompted, enter the user credentials before signing in.

For more information about configuring access to StoreFront through Citrix Gateway, see:

Configure and manage stores

Integrating StoreFront with Citrix Gateway

Google policy

Starting with Citrix Workspace app Version 1909 for Android, you can configure Citrix Workspace app from the Google Admin Console using the Google policy. This feature is supported on Chromebook devices only.

Using the Google policy, you can add one or more stores by adding the store URL.

Known issues:

- This feature is not supported on Android Version 5.0 and earlier.
- When you download the ICA file from a web browser and launch the session, the store added using the Google policy is not applied. Instead, Citrix Workspace app launches the downloaded ICA file.

Sample file of Google policy:

```
{

  "v1": {

    "stores": [
      {

        "url": <"https://xyz.example.com>
        "is_web_interface_enabled":false
       }
 ,
     {

        "url": <https://xyz.example.com>
        "is_web_interface_enabled":false
       }

    ]
   }

 }

<!--NeedCopy-->
```

> **Note:**
>
> Provide the complete store URL and not only the name of the domain.

Email-based account discovery

You can configure Citrix Workspace app to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Citrix Workspace app for Android installation and configuration.

Citrix Workspace app for Android determines the Citrix Gateway or StoreFront server associated with the email address based on Domain Name System (DNS) Service (SRV) records. It then prompts the user to sign in, to access their hosted applications, desktops, and data.

Provision file

You can use StoreFront to create provisioning files that have connection details for accounts. You can make these files available to your users to enable them to configure Citrix Workspace app for Android

automatically.

After installing Citrix Workspace app for Android, users simply open the **.cr** file on the device to configure Citrix Workspace app for Android. If you configure Workspace for websites, users can also get Citrix Workspace app for Android provisioning files from those sites.

For more information, see the StoreFront documentation.

Provide users with account information to enter manually

When you provide users with account details that they need to enter manually. Also, make sure that you distribute the following information to enable them to on connect to their hosted desktops successfully:

- The StoreFront URL or XenApp and XenDesktop Site hosting resources; for example: servername.company.com.
- To access using Citrix Gateway, provide the Citrix Gateway address and required authentication method.

  See the Citrix Gateway documentation for more information.

When a user enters the details for a new account, Citrix Workspace app attempts to verify the connection. If successful, Citrix Workspace app prompts the user to log on to the account.

Provide access to Citrix Virtual Apps and Desktops

Citrix Workspace app requires configuration of StoreFront to deliver apps, desktops, and files from your Citrix Virtual Apps and Desktops deployment.

StoreFront

You can configure StoreFront to provide authentication and resource delivery services for Citrix Workspace app. This enables you to create centralized enterprise stores to deliver:

- Desktops and applications through Citrix Virtual Apps and Desktops.
- XenMobile Apps and mobile apps you have prepared for your organization through XenMobile.

Authentication between Citrix Workspace app and a StoreFront store can be handled using various solutions:

- Users inside your firewall can connect directly to StoreFront.
- Users outside your firewall can connect to StoreFront through Citrix Gateway.
- Users outside your firewall can connect through Citrix Gateway to StoreFront.

Connecting to StoreFront

Citrix Workspace app for Android supports launching sessions from Workspace for Web, if the web browser works with Workspace for Web. If launches do not occur, configure your account through Citrix Workspace app for Android directly.

> **Tip**
>
> When Workspace for Web is used from a browser, sessions are not launched automatically when downloading an **.ICA** file. The **.ICA** file must be opened manually, right after it's downloaded for the session to be launched.

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Workspace app. Create stores that count and aggregate desktops and applications from XenDesktop sites and XenApp, making these resources available to users.

For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Workspace app for Android.

Configure stores for StoreFront just as you would Citrix Virtual Apps and Desktops. No special configuration is needed for mobile devices.

Connect through Citrix Gateway

Citrix Workspace app for Android supports Citrix Gateway 11 and later with access to:

- XenApp and XenDesktop Sites
- StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 and 3.11 stores

You can create multiple session policies on the same virtual server depending on the following:

- the type of connection (such as ICA, clientless VPN, or VPN)
- the type of Workspace deployment (Workspace for Web or locally installed Citrix Workspace app).

The policies can be achieved from a single virtual server.

When your users create accounts on Citrix Workspace app, they need to enter their email address or the matching FQDN of your Citrix Gateway server. For example, if the connection fails when using the default path, enter the full path to the Citrix Gateway server.

Citrix Endpoint Management

Workspace app enables users to access apps, files, and other resources delivered by Citrix Endpoint Management. For more information, see Integration with Citrix Workspace experience

Configure

January 25, 2022

Per-store microphone access

The client-selective trust feature allows Citrix Workspace app to trust access from a VDA session. You can grant access to local client drives and hardware devices like microphones and webcams.

Previously, your setting for microphone access was applied on all configured stores.

Starting with this release, Citrix Workspace app requires the user's permission to access the microphone. The selected setting for microphone access is applied on a per-store basis.

You can configure the access levels from **Settings** > **Store Settings**.

Under the **Set permissions for** option, select the store from the drop-down menu. Enable **Microphone**.

Per-store location access

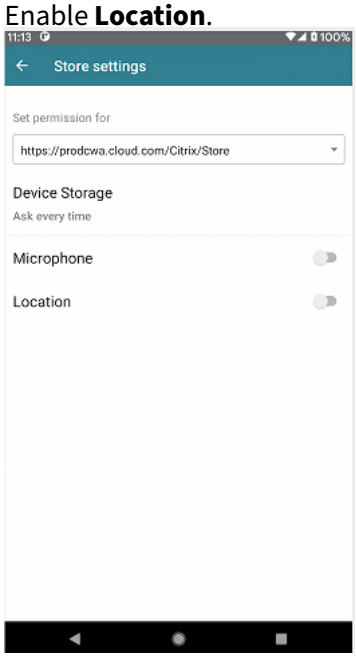
The client-selective trust feature allows Citrix Workspace app to trust access from a VDA session.

Previously, your setting for location access was applied on all configured stores.

Starting with 21.3.0 release, Citrix Workspace app requires the user's permission to access the location. The selected setting for location access is applied on a per-store basis.

Configure the access levels as follows:

1. Select **Settings** > **Store settings**.
2. Under the **Set permissions for** option, select a store from the drop-down menu.
3. Enable **Location**.



VPN functionality

You can access the internal Web, Software-as-a-Service (SaaS) apps, and websites hosted by your company - regardless of your access location. You can access these resources, hosted by your company, without a VPN connection. This feature is available only for customers on cloud stores.

Feature flag management

If an issue occurs with Citrix Workspace app in production, we can disable an affected feature dynamically in Citrix Workspace app even after the feature is shipped. To do so, we use feature flags and a third-party service called LaunchDarkly. You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements.

You can enable traffic and communication to LaunchDarkly in the following ways:

Enable traffic to the following URLs

- events.launchdarkly.com
- stream.launchdarkly.com

- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com
- app.launchdarkly.com

List IP addresses in an allow list

If you must list IP addresses in an allow list, for a list of all current IP address ranges, see LaunchDarkly public IP list. You can use this list to ensure that your firewall configurations are updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the LaunchDarkly Statuspage page.

LaunchDarkly system requirements

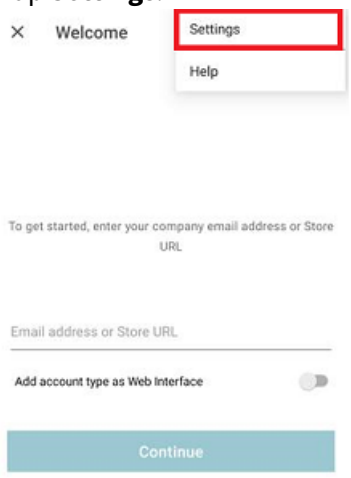
Ensure that the apps can communicate with the following services if you have split tunneling on Citrix ADC set to OFF for the following services:

- LaunchDarkly service.
- APNs listener service

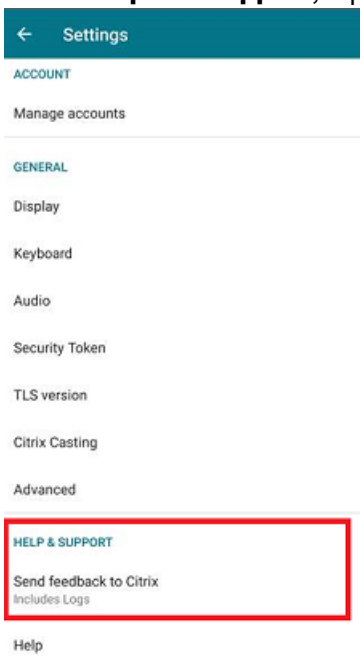
How to collect logs

To collect logs, follow these steps.

1. Tap **Settings**.

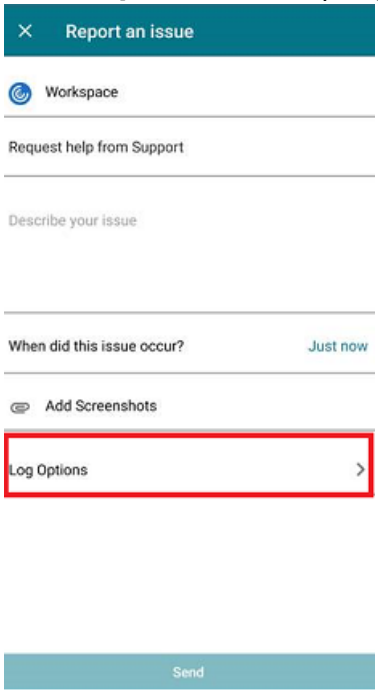


2. Under **Help and Support**, tap **Send feedback to Citrix** (Includes logs).

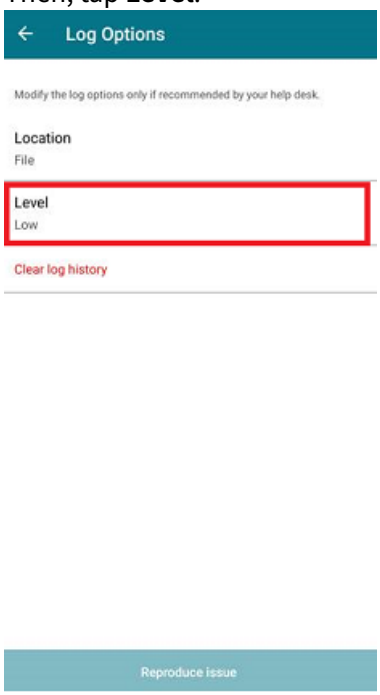


3. Tap **Workspace**.

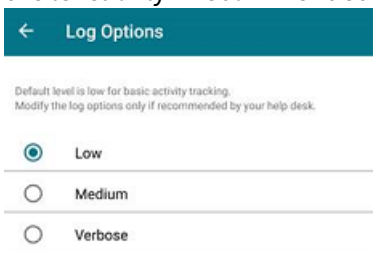
4. Under **Report an issue**, tap **Log Options**.



5. Then, tap **Level**.



6. Select **Low**, **Medium**, or **Verbose** level. (Default level is low for basic activity tracking. Modify the level only if recommended by your help desk).



Auto-launch of ICA file

You can launch your published apps and desktops by clicking the resource. This feature requires StoreFront (on-premises) Version 1912 or later.

> **Note:**
>
> - Auto-launch of ICA file is supported only on Chromebook devices and only for HTTPS store URLs.
> - Don’t select the **Remember my choice** option when you launch a resource.

Enhanced session launch

Published apps and desktops are launched in separate windows. This helps you to use and interact with the store enumeration window without having to disconnect or log off from the session.

> **Note:**
>
> - This feature is supported only on Chromebook devices.
> - This feature is not supported on tablets, phones, and Samsung DeX.

Limitations:

- After changing any user settings, you must relaunch the session for the changes to take effect.
- Apps and desktop are named 'Workspace' in the taskbar - not after the session.
- Only one session can be used at a time.

Workspace with intelligence

Citrix Workspace app for Android is optimized to take advantage of the upcoming intelligent features when they are released. For more information, see Workspace Intelligence Features - Microapps.

Mobile Workspace Experience

The Mobile Workspace Experience uses the Citrix Workspace app to enroll devices through Citrix Endpoint Management.

The Mobile Workspace Experience provides a great end user experience as follows:

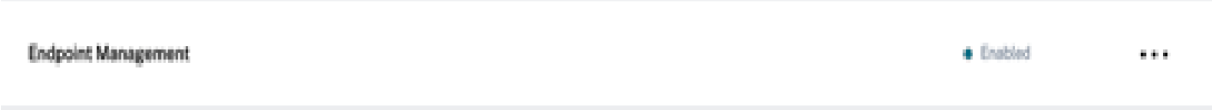
- Enrollment: You can complete the entire enrollment in the Citrix Workspace app itself without using Citrix Secure Hub. In just a few taps, your device gets enrolled in Android Enterprise through Citrix Endpoint Management.
- Security: The Mobile Workspace Experience provides mVPN (mobile virtual private network) connectivity for native apps. Citrix Secure Mail and Secure Web both run on Mobile App Management (MAM) SDK.

> **Note:**
>
> After enrollment, you'll be on Work profile mode, which enables complete separation of personal apps and work apps. Your privacy is maintained as IT only controls Work profile. So, when you're working on your BYOD (bring-your-own-device), you have complete privacy.

As an administrator, configure as follows:

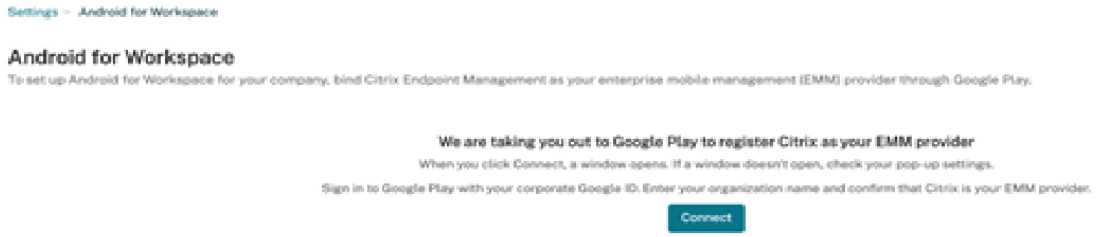
Enable Workspace for Citrix Endpoint Management in Citrix Cloud

1. Sign in to Citrix Cloud.
2. In the upper-left menu, select **Workspace Configuration > Service Integration**.
3. Tap the three dots to the right of Endpoint Management and select **Enable** to enable integration with Citrix Workspace.



Enable Android for Workspace in Settings

1. In Citrix Cloud, select **Settings > Android for Workspace >** and then tap **Connect** to sign in to Google Play with your corporate Google ID.
2. Once registration is complete, you can publish the apps under Android for Workspace.



Enhanced Enrollment profile

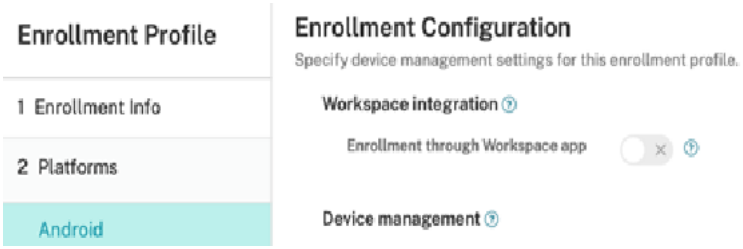
Citrix Endpoint Management supports a feature called Enrollment profile. The feature lets administrators configure different enrollment modes, such as EP2, Work profile, and Personal profile. Administrators configure different enrollment modes, based on delivery groups, on a single server. The feature then assigns these modes to users based on their requirements.

To date, the feature let you configure different Android Enterprise and Device Administrator Legacy modes.

Starting with 21.6.0 release, the Enrollment profile supports additional modes for the Workspace mobile experience. We've modified Citrix Workspace app to consume this API to determine which modes a user requires.

Enable Enrollment profile

In Citrix Cloud, enable Workspace Integration by turning ON **Enrollment through Workspace app** for the appropriate delivery group.



Battery status indicator

The battery status of the device is now displayed in the notification area of a Citrix Desktop session.

> **Note:**
>
> Battery status indicator is not displayed for server VDA.

Client drive mapping

Citrix Workspace app informs the server of the available client drives. By default, client drives are mapped to server drive letters so they appear to be directly connected to the session. These mappings are available only for the current user during the current session.

> **Note:**
>
> This feature is supported only on versions of Android running SDK version 24 and later.

Client drive mapping (CDM) allows plug-and-play storage devices in a session. This means that you can use mass storage devices (For example, pen drives), to copy and paste documents between the pen drive and the user device.

Feature limitations:

- Android APIs are observed to be slow, which delays certain operations.
- CDM for external storage is not supported on Pixel devices.
- File type association is not supported on external storage devices.

Known issue in the feature:

- The Workspace app screen might shift between foreground and background when you plug in an external storage device.

Client Drive Mapping enhancement

Earlier, a selected choice of device storage was applied on all configured stores.

Starting with the release 20.8.0, Citrix Workspace app allows you to select dedicated device storage for every configured store.

You get a prompt to select the type of device storage along with the store details at session launch. You can do one of the following:

- Select one of the device storage options and click **OK** - The choice is applied only to the current session. A prompt appears to select the type of device storage at every launch.
- Select one of the device storage options, select **Do not ask again** and click **OK** - The choice is applied for all session launches for that store. No further prompts appear.
- Select **Cancel** - You are prompted to select a type of device storage at every launch and within a session as well. The session does not have access to the device storage.

> **Note:**
>
> This feature applies only on direct ICA launches and Citrix Gateway configured stores. Stores without end-to-end SSL setup are not supported.

Embedded Citrix HDX RealTime Media Engine

Starting with 20.3.0, the Citrix Workspace app consumes Version 2.9 of the Citrix HDX RealTime Media Engine (RTME).

> **Note:**
>
> You do not need to install HDX RTME to use Skype for Business, you only need the Citrix Workspace app. If HDX RTME is already installed on the Chromebook device, you must uninstall it.

To enable HDX RTME from the Citrix Workspace app:

By default, this setting is set to **Off**.

To enable the HDX RTME from the Citrix Workspace app, go to **Settings** > **Advanced** and select **Enable RealTime Media Engine**.

This feature is supported on:

- Chromebooks running on x86 processors.
- Devices running on Android 6.0 or later.

> **Note:**
>
> Only Citrix Workspace app is needed to use Skype for Business. You do not need to install HDX RTME. If HDX RTME is already installed on the Chromebook device, you must uninstall it.

For more information, see the HDX RealTime Optimization Pack 2.9 documentation.

Unauthenticated users

Citrix Workspace app supports unauthenticated (anonymous) users. Anonymous users can launch Citrix Virtual Apps and Desktops sessions successfully.

USB device redirection

Starting with Version 20.9.0, the USB redirection feature is fully functional and ready for general availability. By default, the USB redirection feature is disabled.

The generic USB redirection feature allows the redirection of arbitrary USB devices from client machines to Citrix Virtual Apps and Desktops. This feature allows you to interact with a wide selection of generic USB devices in a session as if they were physically plugged into it.

As a prerequisite to manage this feature using the Citrix Global App Config Service, set the USB redirection feature to **Enabled** on the Delivery Controller. For more information on how to configure USB redirection on the Delivery Controller, see the Generic USB devices section in the Citrix Virtual Apps and Desktops documentation.

The Citrix Global App Configuration Service gives Citrix administrators the ability to deliver Citrix Workspace service URLs and Citrix Workspace app settings through a centrally managed service.

The USB redirection feature is integrated with and configurable through the Citrix Global App Config Service. You can manage the feature using the Citrix Global App Config Service for non-domain joined networks.

For information on configuring the feature using this method, see Global App Configuration Service in the developer's documentation.

> **Note:**
>
> This feature is ready for general availability starting with Version 20.9.0. In Versions 20.8.1 and earlier, it is available on-demand only.

The USB redirection policy must be set to **Allowed** on the Delivery Controller. For information about configuring USB redirection in Citrix Studio, see Configure generic USB redirection in the Citrix Virtual Apps and Desktops documentation.

For printers and scanners:

Install the vendor-specific drivers on the device. When the installation is complete, the vendor software might ask you to reconnect the USB device. Reconnect the USB device to redirect it.

For Chromebooks:

By default, USB devices (for example, pen drives) are blocked by the Chrome operating system. You must allow the list of devices using the Google admin console for managed Chromebooks.

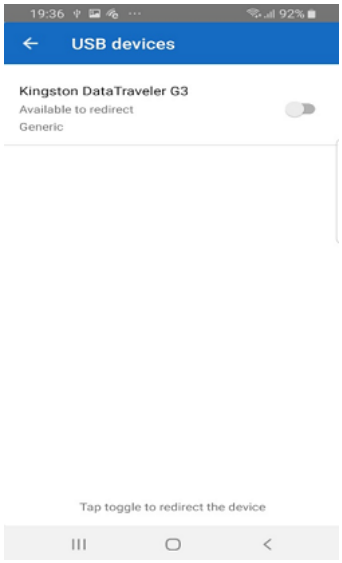
For information on how to allow list of USB devices in a Chromebook, see Knowledge Center article CTX200825.

> **Note:**
>
> Depending on the redirected USB device and the network latency, it might take some time for the device to be visible in the Windows Explorer.

Configuring USB redirection on mobiles phones, tablets, and Samsung DeX

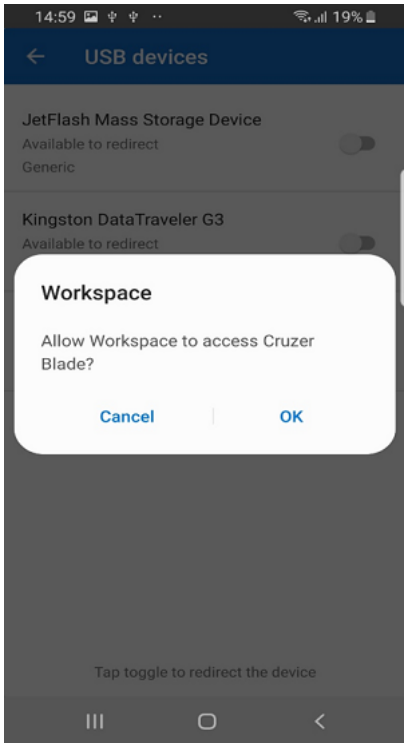
1. Add a USB redirection policy-enabled store and launch a session.
2. Click the session toolbar icon as displayed in the dialog below:

3. Click the **USB Icon** in the session toolbar.
4. Connected USB devices are listed in the USB devices window as shown below:



5. To redirect a particular USB device, click the Toggle option against the device.

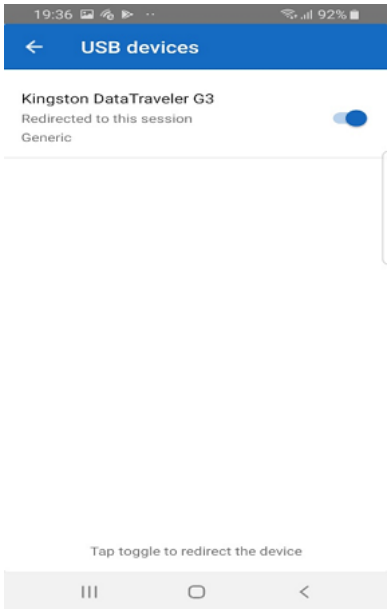
   A Workspace permission dialog appears.



6. Click **OK** to grant permission for the Citrix Workspace app to redirect the device.

   > **Note:**
   >
   > This step is mandatory to redirect the USB device.

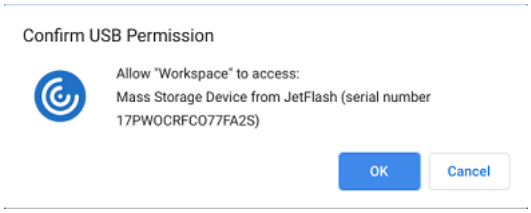
   The USB device is redirected and the status is displayed as shown below:



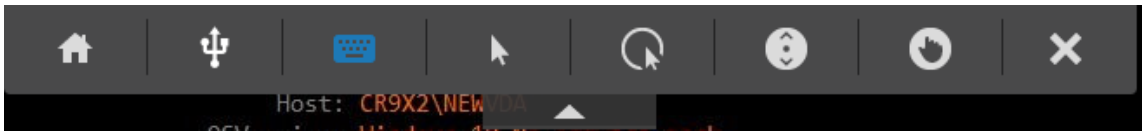
Configuring the USB redirection feature on Chromebooks

1. Add a USB redirection policy-enabled store and launch a session.
2. Click **OK** to grant permission for the Citrix Workspace app to redirect the device.

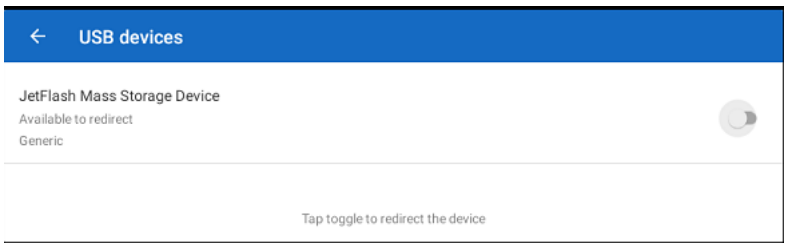
   > **Note:**
   >
   > Granting permission is a mandatory step and the prompt appears only on a fresh install.

3. Connect the USB device.
4. Click the toolbar icon and then the USB icon on the session toolbar.

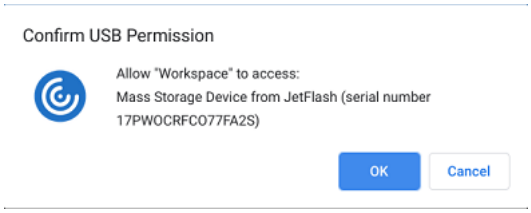
   Connected USB devices are listed as shown below:



> **Note:**
>
> If a USB device isn't listed, ensure that you have whitelisted it.

For information on how to allow list of USB devices on a Chromebook, see Knowledge Center article CTX200825.

5. To redirect the USB device, click the **Toggle** option against the device to be redirected.
6. Click **OK** to grant permission for the Citrix Workspace app to redirect the device.



The USB device is redirected and the status is updated. Dismiss the dialog to continue using the redirected USB device.

> **Note:**
>
> - If a pen drive is redirected, it appears as listed in a session.
> - If a printer or scanner is redirected, it is displayed in the **Devices** section in the control panel.

Tested USB devices

Device	Manufacturer	Model
Printer	HP	LaserJet P2014
Scanner	HP	Scanjet G3010
Scanner	Canon	CanoScan LiDE 700F
Space Navigator	3Dconnexion	
Printer	Brother	QL-580N
Scanner	HP	Scanjet 200

Known issues:

- Only one USB device is supported at a time.
- Audio and video USB devices are not currently supported.

Auto-redirection of USB devices

Citrix Workspace app lets you redirect USB devices automatically when you connect them. When you connect a USB device, a prompt appears, asking you for permission. After you grant the permission, the USB device is redirected automatically.

> **Note:**
>
> This feature is available on-demand only and supports only if the USB device redirection feature is enabled.

Citrix Casting

Citrix Casting combines digital and physical environments to deliver apps and data within a secure smart space. The complete system connects devices (or things), like mobile apps and sensors, to create an intelligent and responsive environment.

Citrix Ready workspace hub is built on the Raspberry Pi 3 platform. The device running Citrix Workspace app connects to the Citrix Ready workspace hub and casts the apps or desktops on a larger display.

Using Citrix Casting, you can:

- Roam your session without launching a VDA session on the mobile devices.
- View the list of available workspace hubs by tapping **View hub list** from the **Workspace hub** dialog.

Configure Citrix Casting

Citrix Casting is enabled when all the following system requirements are met:

- Citrix Workspace app 1809 for Android or later installed
- Bluetooth enabled
- Location enabled
- Mobile device and workspace hub using the same Wi-Fi network

To turn on the Citrix Casting feature, tap **Settings** and **Citrix Casting** on your device.

For more information about the Citrix Ready workspace hub in Citrix Workspace app, see Configure the Citrix Ready workspace hub.

For information about the Citrix Ready workspace hub, see Citrix Ready workspace hub documentation.

Content Collaboration Service integration

Citrix Content Collaboration (formerly ShareFile) enables you to easily and securely exchange documents, send large documents by email, and securely handle document transfers to third parties. There are many ways to work using Citrix Content Collaboration, including a web-based interface, mobile clients, desktop apps, and integration with Microsoft Outlook and Gmail.

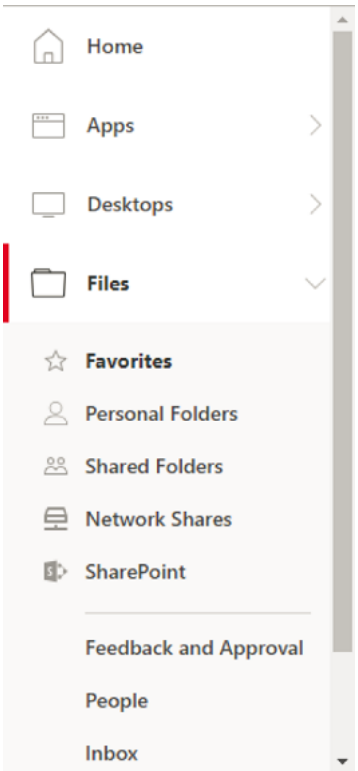
You can access Citrix Content Collaboration using the **Files** tab in the Citrix Workspace app. You can view the **Files** tab only if the Content Collaboration Service is enabled in the Citrix Cloud console. For information, see Create or link a Content Collaboration (ShareFile) account to Citrix Cloud.

> **Note:**
>
> Citrix Content Collaboration integration is not supported on Windows Server 2012 and Windows Server 2016 due to a security option set in the operating system.

Feature limitations:

- Resetting Citrix Workspace app does not cause Citrix Content Collaboration to log off.
- Switching stores in Citrix Workspace app does not cause Citrix Content Collaboration to log off.

The following image displays example contents of the **Files** tab of the Citrix Workspace app:



Keyboard layout synchronization

Citrix Workspace app offers separate options to enable the client IME and keyboard layout synchronization under **Settings**.

The **Enable client IME** option allows you to type the double-byte characters (such as Chinese, Japanese, and Korean characters) directly at the insertion point in a session.

The **Sync Keyboard** option allows automatic keyboard layout synchronization between the VDA and the client device.

On a fresh install and by default, the **Enable client IME** option is set to **On** for Japanese, Chinese, and Korean languages and the **Sync Keyboard** option is set to **Off**.

To enable dynamic keyboard layout synchronization, set both the **Enable client IME** and **Sync Keyboard** options to **On**.

Note:

- The VDA must be version 7.16 or later.
- Administrators must enable the enhanced support for Asian languages feature on the VDA. By default, the feature is enabled. However, on Windows Server 2016 VDA, you must add a new key called **DisableKeyboardSync** and set the value to 0 in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme` to enable the feature.
- Administrators must enable the unicode keyboard layout-mapping feature on the VDA. By default, the feature is disabled. To enable it, create the **CtxKlMap** key under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` and set DWORD value EnableKlMap = 1 under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap`.

Feature Limitations:

- This feature works only on soft keyboards on the devices, not on external keyboards.
- Certain mobile devices might not fully support keyboard layout synchronization, such as the Nexus 5x
- The keyboard layout can only be synced from the client to the server. When changing the server-side keyboard layout, the client keyboard layout cannot be changed.
- When you change the client keyboard layout to a non-compatible layout, the layout might be synced on the VDA side, but functionality cannot be confirmed.
- Remote applications that run with elevated privileges (for example, applications you run as an administrator) can't be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the VDA or disable UAC.

USB smart card

Citrix Workspace app provides support for USB smart card readers with StoreFront. You can use USB smart cards for the following purposes when enabled:

- Smart card logon - Authenticates users to Citrix Workspace app.
- Smart card application support - Enables smart card-aware published applications to access local smart card devices.

Citrix Workspace app supports this feature on all Android devices listed by Biometric Associates.

Citrix Workspace app supports the following types of USB smart cards:

- Personal Identity Verification (PIV) cards
- Common Access Cards (CAC) cards

USB smart card is supported on Android operating system 6.0(Marshmallow) to Version 7.12(Nougat). Android operating system Version 8.0(Oreo) and 9.0(Pie) are not supported. This is a third-party limitation.

You can also enable USB smart card authentication from **Settings** > **Manage Accounts**.

Configuring USB smart card

Prerequisite:

- Download and install the Android PC/SC-Lite service from the Google Play Store.

1. Connect the USB smart card reader to the mobile device. For information about connecting smart card readers, refer to the smart card reader specifications provided by the manufacturer.
2. Add a smart card enabled StoreFront account.
3. On the Citrix Workspace app logon page, tap **Add Account**. Tap the **Use Smartcard** option.
4. To edit an existing account to use the USB smart card authentication, tap **Accounts** > **Edit** and tap the **Use Smartcard** option.

File type association

As a prerequisite for this feature to work, go to the Citrix Workspace app settings and set the **Use device storage** option to **Full Access**. An additional option, **Ask every time** is also available so that you are prompted for permission before accessing your device storage in a session.

> **Note:**
>
> **Ask every time** option is a per-session setting. It does not carry forward to the next session.

When you select **Ask every time**, any system-generated access to your device storage might cause the **Use device storage** prompt to appear (for example, at logoff). This is expected behavior.

Citrix Workspace app reads and applies the settings configured by administrators in Citrix Studio. To apply FTA in a session, ensure that users connect to the Store server where the FTA is configured.

On the user device, select the file you want to launch File Explorer and click Open. The Android operating system provides an option to launch the file using Citrix Workspace app (applying the FTA

configured by the administrator) or a different application. Depending on your earlier selection, a default application might or might not be set. You can change the default application using the Change default option.

> **Note:**
>
> This feature is available only on StoreFront and requires Citrix Virtual Apps and Desktops Version 7 or later.

File type association (FTA) with Google Drive

When using a Chromebook, you can access files residing on Google Drive from Citrix Workspace app using the file type association (FTA) feature. You can seamlessly use Android applications available on Chromebooks to access these files. For example, if you save a .doc file to Google Drive, you can open the file using an Android application (in this case, Microsoft Word) on the Chromebook from within Citrix Workspace app.

> **Note:**
>
> Only Chromebook devices support FTA with Google Drive.

Enabling access to files on Google Drive:

1. Download the Citrix File Access component (FileAccess.exe) from the Citrix Workspace app for Chrome download page and install it on the VDA.
2. Using Citrix Studio, configure the appropriate file type associations (FTAs) for published applications. FTAs can be configured from the respective application properties or settings. For more information about how to set FTA, see Knowledge Center article CTX218743.
3. In a Citrix Virtual Apps and Desktops session, open the default browser, add the following URL to the trusted sites: `https://accounts.google.com` and `https://ssl.gstatic.com`.
4. On the Chromebook device, select the file you want to launch. Tap **Open** and select Citrix Workspace app from the list.

Known issues and limitations in the feature

1. Smart card authentication might be slower than password authentication. For example, after disconnecting from a session, wait for approximately 30 seconds before attempting to reconnect. Reconnecting to a disconnected session too quickly might cause Citrix Workspace app to turn unresponsive.
2. Smart card authentication is not supported on farms.
3. Some users might have a global PIN number for smart cards; however, when users log on using a smart card account, they must enter the PIV PIN and not the global smart card PIN. This is a third-party limitation.

4. Citrix recommends that you exit and restart the Citrix Workspace app session after you log off from the smart card account.
5. Multiple USB smart cards are not supported.
6. You can access only MIME file formats supported by Microsoft Office, Adobe Acrobat reader and Notepad applications using the file type association feature.

Customer Experience Improvement Program (CEIP)

Data collected	Description	What we use it for
Configuration and usage data	The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app and automatically sends the data to Google Analytics for Firebase.	This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app.

Additional Information

Citrix will handle your data in accordance with the terms of your contract with Citrix, and protect it as specified in the Citrix Services Security Exhibit available on the Citrix Trust Center.

You can disable sending CEIP data to Citrix and Google Analytics for Firebase (except for the two data elements collected for Google Analytics for Firebase indicated by an * in the following table) by:

1. Launch the Citrix Workspace app and select **Settings**.
2. Select **Advanced Preferences**.

   The **Advanced Preferences** dialog appears.
3. Clear the option **Send Usage statistics**.

The specific CEIP data elements collected by Google Analytics for Firebase are:

Operating system version*	Workspace app version*	Authentication configuration	Device information
Session launch method	Citrix store type	Client drive-mapping configuration	

Session information	`Recieverconfig.txt` usage	USB redirection configuration	HDX RTME user info
HTTP and HTTPS connection configuration	ICA connections protocol info	Workspace app review action	Disable Firebase Configuration
Number of stores added	Screen capture action	RSA feature user actions	StoreFront Vs Workspace app user count
App update action	Operating system update	Screen view action	App remove
Web view connections	App clear data	App execution	App session start

Security settings

Citrix recommends using stores that are secure. Besides, it is a good practice to have HTTP strict transport security (HSTS) setting enabled for secure stores.

Perform the following steps to enable the HSTS setting:

1. In **Citrix StoreFront**, under **Stores**, click on the link of the particular store to enable the security settings.
2. The **Manage Receiver for Web Sites** dialog box appears.
3. Click **Configure**.
4. The **Edit Receiver for Web site** dialog box appears.
5. Click the **Advanced Settings** tab and select **Enable strict transport security**.

User experience

Option to disable display of error messages

You can now disable the display of the following error message related to network monitoring:

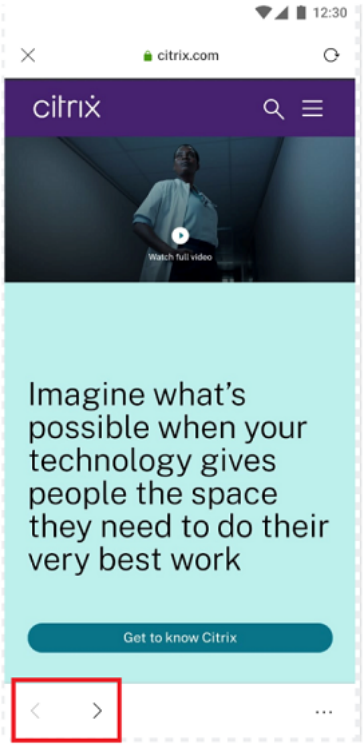
“Connection might be temporarily slow.”

To disable the error message relating to network issues in a session, go to **Advanced** and select the **Disable network monitoroting messages** option.

User interface enhancement

- Starting with 20.7.0 release, you can remove the store account details from the **Edit** option. Click **Remove account** to remove the account details.
- Starting with 20.7.5 release, the **Recent** tab displays the native mobile apps along with the published apps and desktops.
- Starting with 20.10.0 release, Citrix Workspace app supports Google Play's current target API requirements for Android 10.
- Starting with 20.10.0 release, you receive a notification about a non-secure connection when you try to add an HTTP store.
- Starting with 21.3.5 release, you can navigate back and forth within web and Software-as-a-Service (SaaS) apps, as well as from the microapp view.

  The navigation buttons appear at the bottom left of your workspace web and SaaS app session of your mobile phone.

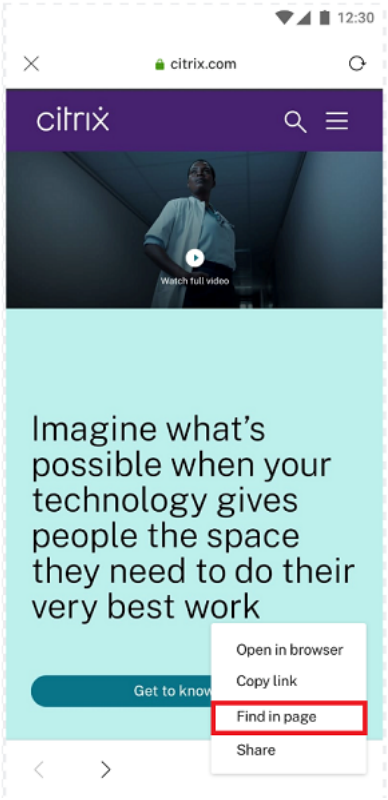


  The navigation buttons appear at the top left of your SaaS app session of your tablet.

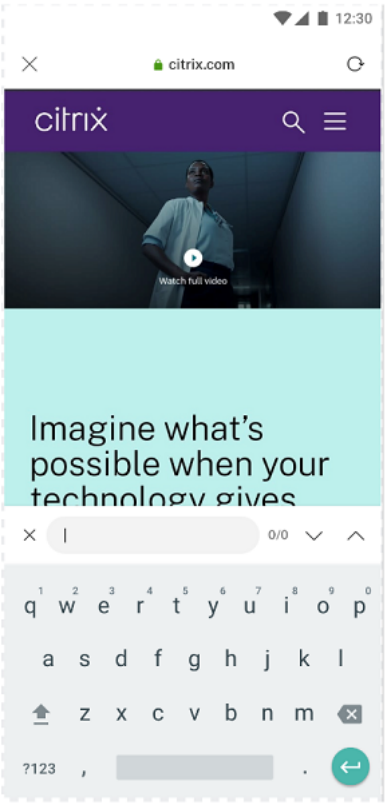
- Starting with 21.4.0 release, you can search for words or phrases within your web and Software-as-a-Service (SaaS) apps.

  To search, follow these steps.

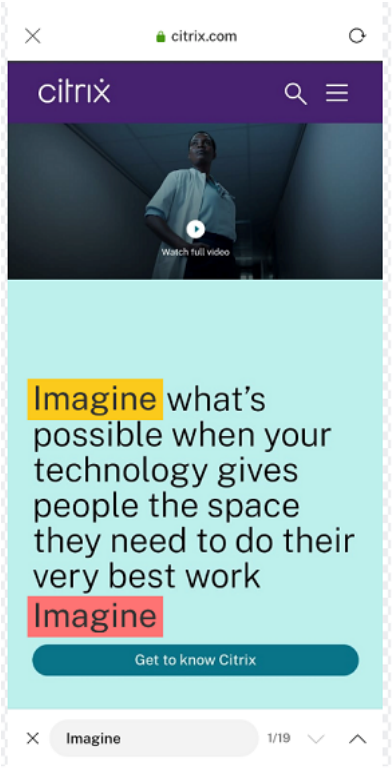
1. Tap the ellipsis button on the bottom right and select **Find in page**.



2. The keyboard appears.



3. On typing, your search result appears (for example, the word “imagine”).



- Starting with 21.6.0 release, you can download text, audio, and video files (with and without direct links). For text, audio, and video files with direct links, download directly by tapping the link. You can preview the audio and video files before downloading them.

  To download files without direct links, tap the ellipsis button on the bottom right and select **Download.**

After the download completes, a notification indicates that the file is saved in your downloads folder.

- Starting with 21.8.5 release, we now support Android 12 Beta 4 in Citrix Workspace app for Android. Upgrading to Citrix Workspace app version 21.8.5 ensures uninterrupted support for devices that are updated to Android 12 Beta 4.
- Starting with 21.9.0 release, Citrix Workspace app supports Android 12 Beta 4. If you are on HTTP-based stores, for a secure context, we recommend that you transition to HTTPS-based stores. For more information, see HTTPS.

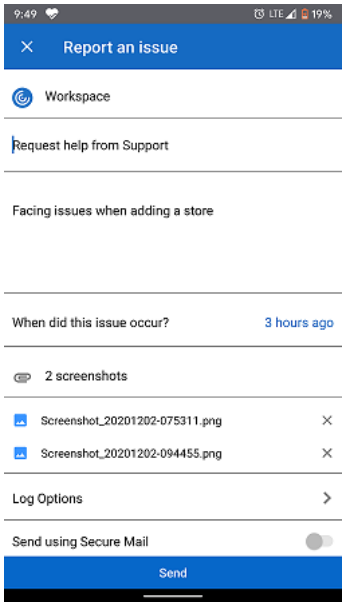
Enhanced feedback mechanism

Previously, you could provide feedback to Citrix using Citrix Workspace app only through email.

Starting with 20.12.0 release, you can send us feedback about Workspace and report issues using the same interface. To send feedback:

Click **Settings** > **Send feedback to Citrix**.

The **Report an issue** dialog appears.



Using the **Report an issue** dialog, you can:

- Request help from Support
- Report an issue
- Send issue logs

Cryptography

This feature is an important change to the secure communication protocol. Cipher suites with the prefix TLS_RSA_ doesn't offer forward secrecy and are considered weak.

The TLS_RSA_ cipher suites have been removed. The releases 20.6.5 and later supports advanced TLS_ECDHE_RSA_ cipher suites. If your environment isn't configured with the TLS_ECDHE_RSA_ cipher suites, you cannot launch the client because of weak ciphers.

The following advanced cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

TLS v1.0 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS v1.2 supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Support for Android Enterprise

Starting with 20.12.0 release, Citrix Workspace app supports Android Enterprise.

For more information, see the Android Enterprise in the Citrix Endpoint Management documentation.

Enlightened Data Transport (EDT)

In earlier releases, session launches were unsuccessful when Enlightened Data Transport (EDT)connections couldn't be established between Citrix Gateway and the VDA. Starting with 21.5.0 release, unsuccessful EDT connections fall back to Transmission Control Protocol (TCP).

EDT stack parameters enabled by default

Starting with 21.7.0 release, the EDT stack parameters are enabled by default. As a result, we've removed the *EDT Stack Parameters* option from **Settings > Advanced**.

To date, the option to disable EDT stack parameters was available to users. With this option available, not all clients were following custom EDT Maximum Segment Size (MSS) requirements consistently. As a result, fragmentation occurred with degradation in HDX performance and issues in establishing sessions for these clients. With EDT stack parameters newly enabled by default, the overall user experience and satisfaction is now enhanced.

Parallel connection

Starting with 21.7.0 release, we've are introducing the EDT and TCP parallel connection feature. The feature results in decreased connection times.

Earlier, when establishing a connection, the Workspace app would try to connect using EDT. Unsuccessful EDT connection attempts would fall back to TCP.

This caused the following issues that are now addressed:

- Increased connection time in fallback scenarios.
- Session reliability and Auto client reconnect tended to favor TCP.
- Required a connection break to try TCP again.

MTU Discovery capabilities added to EDT

We've added Maximum Transmission Unit Discovery capabilities to Enlightened Data Transport (EDT). As a result, you can now enjoy a consistently stable HDX experience, delivered by EDT.

Earlier, EDT could fail in several scenarios such as VPN, Wi-Fi, 4G or 3G connections, and on Microsoft Azure, caused by packet loss due to packet size. When you tried to launch a session, packet fragmentation could cause sessions to drop. As a workaround, it was necessary to adjust the EDT MSS (Maximum Segment Size) in the StoreFront file, which meant extra configuration. The addition of *MTU Discovery capabilities* added to EDT resolves and addresses these issues.

MTU Discovery capabilities added to EDT work in sessions hosted on 1912 VDA and later.

Service continuity Feature preview

> **Note:**
>
> - This feature is in public technical preview.

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services. For more information, see Service continuity section in the Citrix Workspace documentation.

Authenticate

January 25, 2022

RSA SecurID

> **Note:**
>
> Citrix Workspace app has deferred support for **Next Token Mode** because of a third-party dependency. More information about the supportability can be expected as it gets available.

With this feature enabled,

- If you enter three incorrect passwords, the Citrix Gateway plug-in prompts you to wait until the next token is active before sign-in.
- If you have sign-in too many times with an incorrect password, the RSA server can disable your account.

For more information, see the Authentication and Authorization section in the Citrix Gateway documentation.

> **Tip:**
>
> Citrix Secure Web Gateway configurations do not support RSA SecurID authentication. To use RSA SecurID, use Citrix Gateway.

Installing RSA SecurID Software Tokens

An RSA SecurID Software Authenticator file has an `.sdtid` file name extension. Use the RSA SecurID Software Token Converter to convert the `.sdtid` file to an XML-format 81-digit numeric string. Get the latest software and information from the RSA website.

Follow these general steps:

1. On a computer (not mobile device), download the converter tool here. Follow the instructions on the website and the readme included with the converter tool.
2. Paste the converted numeric string into an email and send it to user devices.
3. On the mobile device, make sure that the date and time are correct, which are required for authentication.
4. On the device, open the email and click the string to start the software token import process.

After the software token is installed on the device, a new option appears in the **Settings** list to manage the token.

> **Note:**
>
> On mobile devices that do not associate the `.sdtid` file with Citrix Workspace app, you need to change the file name extension to .xml and then import it.

SDK and API

January 25, 2022

Citrix Virtual Channel Software Development Kit (SDK)

The Citrix Virtual Channel SDK supports writing server-side applications and client-side drivers for other virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops servers.

This version of the SDK supports writing new virtual channels for Citrix Workspace app for Android. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Android Virtual Driver AIDL interfaces: **IVCService.aidl** and **IVCCallback.aidl**, used with virtual channel functions in Citrix Server API SDK (WFAPI SDK) to create new virtual channels.
- A helper class **Marshall.java** designed to make writing your own virtual channels easier.
- Working source code for three virtual channel sample programs that demonstrate programming techniques.

The Virtual Channel SDK requires the WFAPI SDK to write the server-side of the virtual channel. For more information on SDK, see Citrix Virtual Channel SDK for Citrix Workspace app for Android.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States